Tenda®

Model: W307R

# User Guide

www.tenda.cn

Wireless-N
Broadband Router

# Copyright Statement

Tenda® is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without the permission of Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages.

All the photos and product specifications mentioned in this manual are for references only. As the upgrade of software and hardware, there will be changes. And if there are changes, Tenda is not responsible for informing in advance. If you want to know more about our product information, please visit our website at www.tenda.cn.

# Contents

**Chapter 1: Introduction** ..... *1*
Package Contents ..... 1

**Chapter 2: Getting to Know the Wireless-N Broadband Router** ..... *2*
The Rear Panel ..... 2
The Front Panel ..... 3
Hardware Installation ..... *4*

**Chapter 3: Getting to Connect the Wireless-N Broadband Router** ..... *5*
How to Set the Network Configurations for My Computer ..... *5*
How to Check the Network Connection ..... 7

**Chapter 4: Basic Configurations** ..... *9*
How to Access the Web-based Configuration Utility ..... 9
Setup Wizard ..... 10

**Chapter 5: Advanced Settings** ..... *14*
LAN Settings ..... 14
WAN Settings—PPPoE ..... 15
WAN Settings—Static IP ..... 16
WAN Settings—L2TP ..... 167
WAN Settings—PPTP ..... 168
MAC Address Clone ..... 17
DNS Settings ..... 20

**Chapter 6: Wireless Settings** ..... *21*
Wireless Mode ..... 24
Basic Settings ..... 24
Wireless Security Settings ..... 24
WEP ..... 25
WPA-Personal ..... 26
WPA2-Personal ..... 27
WPA-Enterprise ..... 27
WPA2-Enterprise ..... 27
802.1x ..... 28
WPS ..... 31
WDS ..... 31
Advanced Wireless Settings ..... 33
Wireless Access Control ..... 36
Wireless Connection Status ..... 37

**Chapter 7: DHCP Server** ..... *38*
DHCP Server List ..... 39

**Chapter 8: Virtual Server** ..... *40*
Single Port Forwarding ..... 40
Port Range Forwarding ..... 42
Port Trigger ..... 40
ALG Service ..... 40
DMZ Settings ..... 47
UPnP Settings ..... 47

**Chapter 9: Traffic Control** ..... *48*
Traffic Control ..... 48

**Chapter 10: Security Settings** ..... *50*
Client Filter Settings ..... 50
URL Filter Settings ..... 51
MAC Address Settings ..... 52
Prevent Network Attack ..... 53
Remote Web Management ..... 53
Local Web Management ..... 54
Wan Ping ..... 54

**Chapter 11: Routing Settings** ..... *55*
Routing Table ..... 55
Static Route ..... 55

**Chapter 12: System Tools** ..... *55*
Time ..... 56
DDNS ..... 56
Backup/Restore ..... 57
Firmware Upgrade ..... 58
Restore to Factory Default Settings ..... 59
Reboot ..... 60
Change Password ..... 60
System Log ..... 61

**Appendix A: Product Features** ..... *62*

# Chapter 1: Introduction

Thank you for choosing the W307R Wireless-N Broadband Router. It employs the advanced MIMO (Multi Input, Multi Output) technology and integrates router, wireless access point, four-port switch and firewall in one, which will allow you to share Internet access over the four switched ports or via the wireless broadcast. Compatible with IEEE 802.11n (Draft 2.0) standard, it can connect with existing 802.11b/g PCI, USB and Notebook adapters. Up to 300Mbps transmission rate allows you to enjoy real-time activities such as video streaming, online gaming and so on.

Besides, the Wireless-N Broadband Router supports all of the latest wireless security features, such as 64/128-bit WEP encryption, WPS (PBC and PIN) encryption method, packet filtering and port forwarding, to prevent unauthorized access and protect your network against malicious attack.

Moreover, the user-friendly Setup Wizard on the CD-ROM can assist you to set up the Wireless-N Broadband Router easily. It also can be managed or configured through Local/Remote easy-to-use Web-based utility. So it is the best choice for SOHOs and small-sized enterprises.

## Package Contents

- One W307R Wireless-N Broadband Router
- One Ethernet Network Cable
- One Quick Installation Guide
- One Power Adapter
- One CD-ROM

If any of listed items are missing or damaged, please contact the Tenda reseller from whom you purchased for replacement immediately.

# Chapter 2: Getting to Know the Wireless-N Broadband Router

## The Rear Panel

Here is the description of the back panel. The RJ-45 ports for cable connection and Reset button are located on the back panel as shown below.

**Connections:**

| Rear Panel Interface | Description |
|---|---|
| 1-4 (LAN Ports) | Connect to Ethernet devices (such as computers, switches, hubs). |
| RESET/WPS | **Note:** After pressing the RESET button for 7 seconds, the configurations you have set will be deleted and the device will restore to the factory default settings. If you press this button for 1 second, the WPS (PBC) function is enabled. |
| WAN | Connect to DSL Modem, Cable Modem or community broadband |
| POWER | Receptor for the supplied power adapter. |

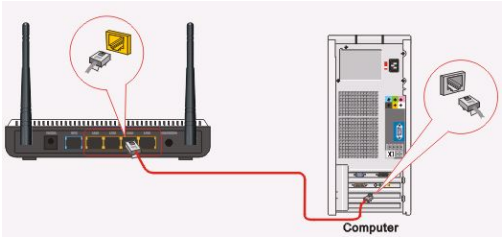
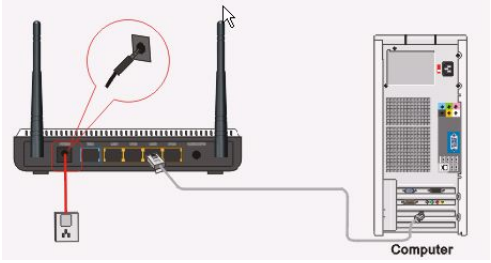
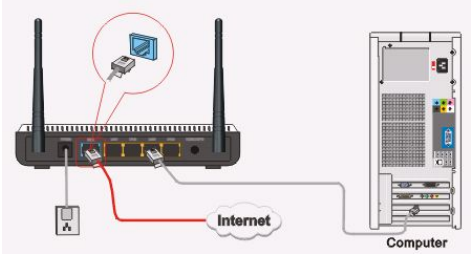
## The Top Panel

There are the Router's LED indicators on the top panel as shown below.

**LEDS:**

| LED Indicator | Status | Description |
|---|---|---|
| POWER | Always ON | The POWER indicator is Always ON when it is powered on and works properly. |
| SYS | Blinking | The SYS is blinking regularly when the system works normally. |
| WAN | Always ON | Indicates the correct connection of the WAN ports. |
| | Blinking | Indicates the Router is transmitting/receiving data packets. |
| WLAN | Blinking | Indicates the wireless signal is OK. |
| LAN(1/2/3/4) | Always ON | Indicates the correct connection of the LAN ports. |
| | Blinking | Indicates the Router is transmitting/receiving data packets. |
| WPS | Blinking | Indicates the Router is negotiating with WPS clients in WPS Mode (PBC or PIN). |

# Hardware Installation

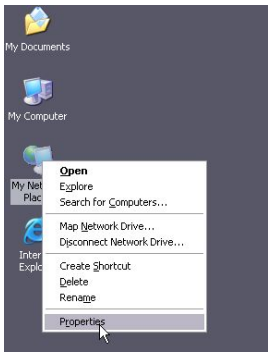
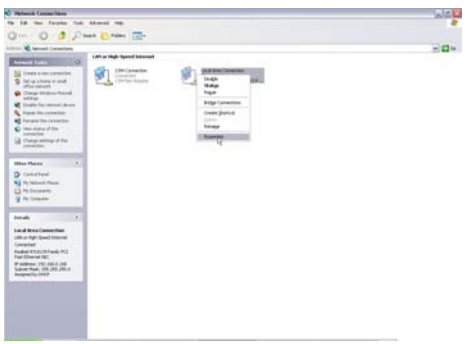
| | |
|---|---|
| 1. Please connect the LAN port of the router to the network adapter of your computer with one cable. |  |
| 2. Please use the delivery-attached power adapter to power the router. |  |
| 3. Please connect your broadband line provided by your ISP to the WAN port of your router. |  |

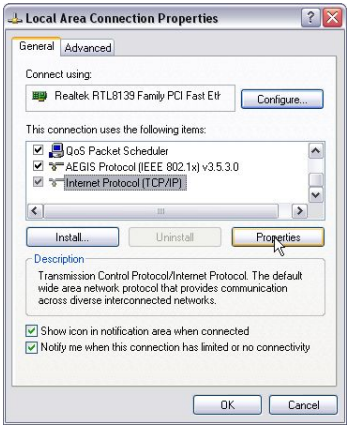
***IMPORTANT:*** ***<u>Please use the included power adapter. Use of a different power adapter could cause damage and void the warranty for this product.</u>***

# Chapter 3: Getting to Connect the Wireless-N Broadband Router

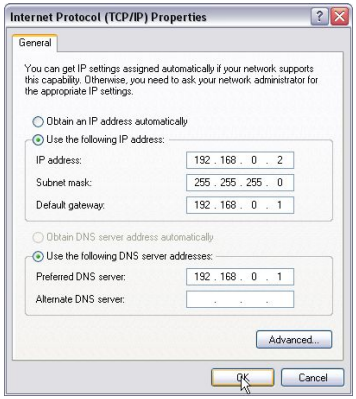
For easy and fast configuration, the following steps for network configuration are required.

## How to Set the Network Configurations for My Computer

| | |
|---|---|
| Right click "**My Network Places**" and select "**Properties**". |  |
| Right click "**Local Area Network Connection**" and select "**Properties**". |  |

| | |
|---|---|
| Select "**Internet Protocol (TCP/IP)**" and click "**Properties**". |  |
| Select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**". Click "**OK**" to save the configurations. | |

**Or** select "**Use the following IP address**" and enter the IP address, Subnet mask, Default gateway as shown right. Of course, you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router's default gateway as the DNS proxy server. Click "**OK**" to save the configurations.

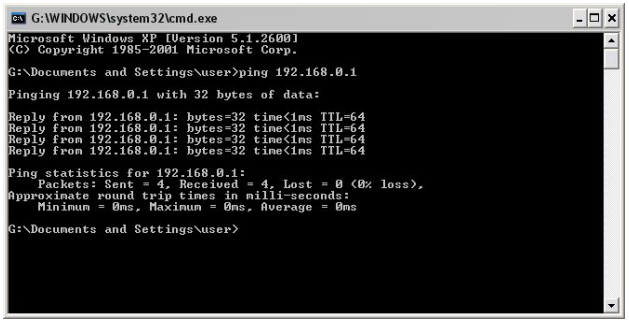

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:
Advanced...
OK
Cancel

## How to Check the Network Connection

Select "**Start**"— "**Programs**"—"**Accessories**" —"**Command Prompt**".

Input the "**ping 192.168.0.1**" and press "**Enter**". If the screen displays as the right figure, it means your PC is connected to your router successfully.

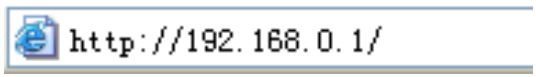
If not, please make sure the hardware installation and network adapter are OK. After all preparations are made, please proceed to Chapter 4 for more and advanced configuration.


G:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
G:\Documents and Settings\user>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
G:\Documents and Settings\user>

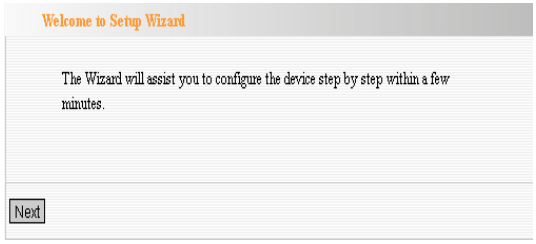
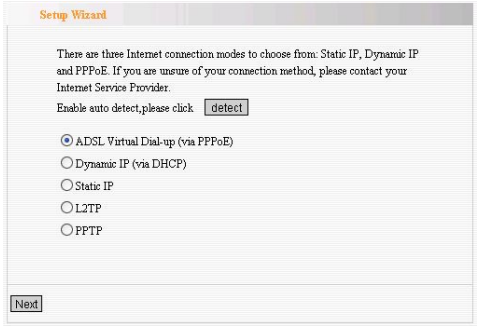
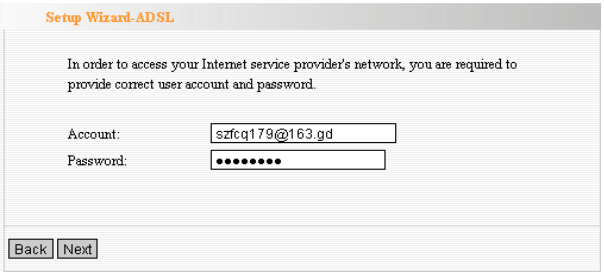
# Chapter 4 Basic Configurations

This section is to show you how to configure your new Wireless-N Broadband Router through the Web-based Configuration Utility.

## How to Access the Web-based Configuration Utility

| | |
|---|---|
| To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, http://192.168.0.1. Press "**Enter**". |  |
| Please input the "**admin**" in both User Name and Password. Click "**OK**". | |

# Setup Wizard

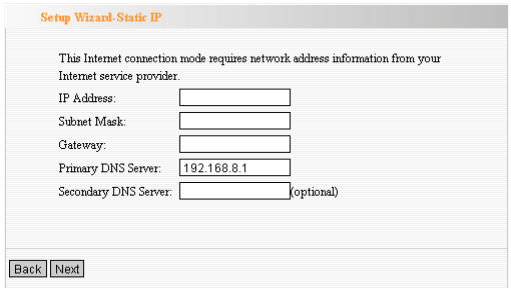
| | |
|---|---|
| Here is the "**Welcome to Setup Wizard**" for configuring your Router quickly. Click "**Next**". |  |
| In this screen, select one mode of your Internet connection you use. If you are not clear, press the "**Detect**" button or contact your Internet Service Provider, and click "**Next**". |  |
| ➔**Connection Mode 1**: ADSL Virtual Dial-up (Via PPPoE)<br><br>Enter the Account and Password provided by your ISP, and click "**Next**". |  |

➔**Connection Mode 2**: Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like Mode 2 or Mode 3.

➔**Connection Mode 3**: Static IP

In this screen, fill the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click "**Next**".




➔**Connection Mode 4**: L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP use a L2TP connection, your ISP will provide you with a username and password please fill in the parameters.

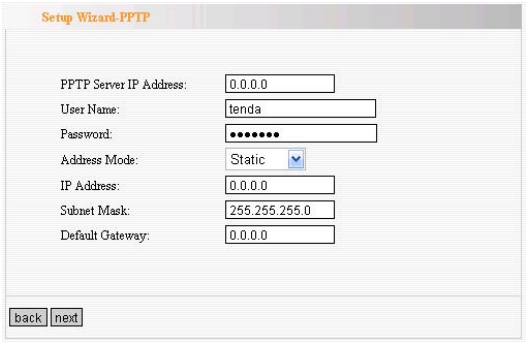
**L2TP provides two access modes.**

If the L2TP offered by your ISP is **Dynamic IP**: Please select Dynamic IP.

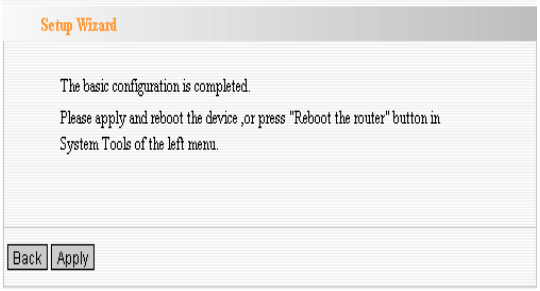
If the L2TP offered by your ISP is **Static IP**: Please fill in the parameters provided by your ISP.
After configuration, please click “Next”.

➔**Connection Mode 5**: PPTP

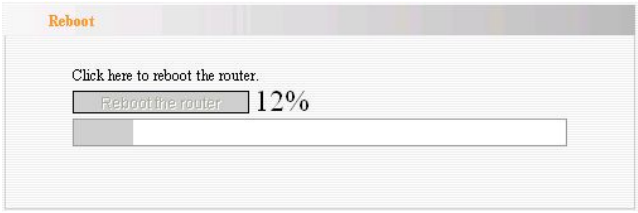
If the connection is “PPP Tunneling Protocol”, please input the following parameters provided by your ISP: Server IP Address, User Name, and Password.
**PPTP provides two access modes.**
If the PPTP offered by your ISP is **Dynamic IP**: Please select Dynamic IP.
If the PPTP offered by your ISP is **Static IP**: Please fill in the parameters provided by your ISP.
After configuration, please click “Next”.




Click “**Apply**”, select “**Reboot**” in **System Tools** of the left menu and press the “**Reboot the router**” button.


Setup Wizard
The basic configuration is completed.
Please apply and reboot the device ,or press "Reboot the router" button in System Tools of the left menu.
Back
Apply

It is rebooting now, please wait for a few minutes and **DO NOT** power off it.




Click the "***System Status***" in the left menu of the Web-based Utility to find out the current network and system information. If the "Connection Status" is "Connected", Congratulations you on completing the Router's basic settings. You are on the Internet now. If you want to configure more, please proceed to the following explanations for Advanced Settings.

# Chapter 5: Advanced Settings

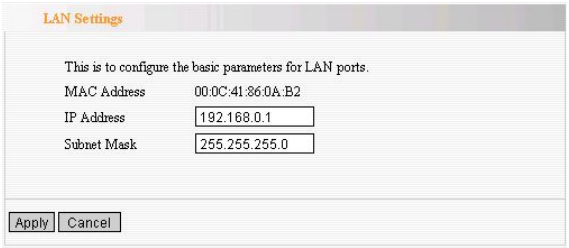
This section is to conduct the advanced configurations for the Router, including LAN Settings, WAN settings, MAC Address Clone and DNS Settings.

## LAN Settings

**MAC Address:** The Router's physical MAC address as seen on your local network, which is unchangeable.

**IP Address:** The Router's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.0.1 is the default value.

**Subnet Mask:** It's shown the Router's subnet mask for measurement of the network size. 255.255.255.0 is the default value.



# WAN Settings—PPPoE

**Connection Mode:** Show your current connection mode.

**Account:** Enter them provided by your ISP.

**Password:** Enter them provided by your ISP.

**MTU:** Maximum Transmission Unit. It is the size of largest datagram that can be sent over a network. The default value is 1492. **Do NOT** modify it unless necessary.

**Service Name:** It is defined as a set of characteristics that are applied to a PPPoE connection. Enter it if provided. **Do NOT** modify it unless necessary.

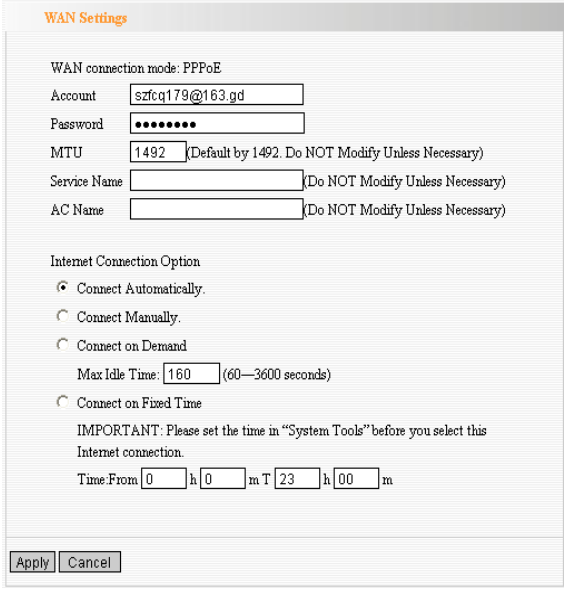
**AC Name:** Enter it if provided. **Do NOT** modify it unless necessary.

Connect automatically to the Internet after rebooting the system or connection failure.

**Connect Manually:** Connect to the Internet by the user manually.

**Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means your Internet connection at all time. Otherwise, enter the minutes to be elapsed before you want to disconnect the Internet access.

**Connect on Fixed Time:** Connect to the



Internet during the time you fix.

## WAN Settings—Static IP

If your connection mode, static IP is chosen, please enter the following addressing information.

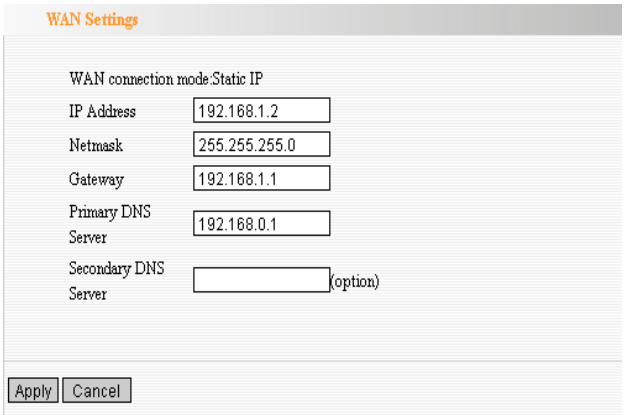
**IP Address:** Here enter the WAN IP address provided by your ISP.

**Subnet Mask:** Enter the WAN Subnet Mask here.

**Gateway:** Enter the WAN Gateway here.

**Primary DNS Server:** Enter the Primary DNS server provided by your ISP.

**Secondary DNS Server:** Enter the secondary DNS



# WAN Settings—L2TP

**L2TP Server IP:** Enter the Server IP provided by your ISP.

**User Name:** Enter L2TP username.

**Password:** Enter L2TP password.

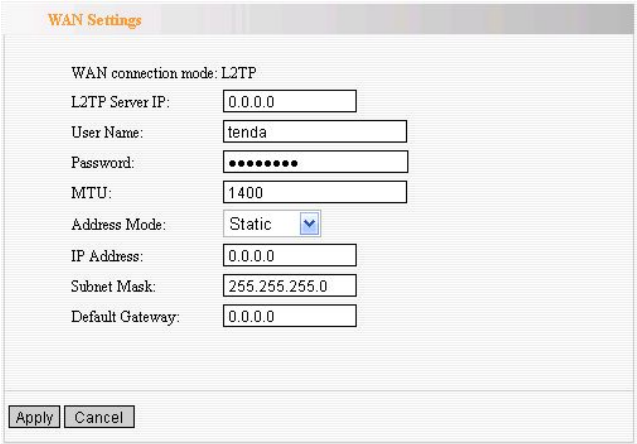
**MTU:** Maximum Transmission Unit, you may need to change it for optimal performance with your specific ISP. 1400 is the default MTU.

**Address Mode:** Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

**IP Address:** Enter the L2TP IP address supplied by your ISP.

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP.

**Default Gateway:** Enter the Default Gateway supplied by your ISP.



# WAN Settings—PPTP

**PPTP Server IP:** Enter the Server IP provided by your ISP.

**User Name:** Enter PPTP username provided by your ISP.

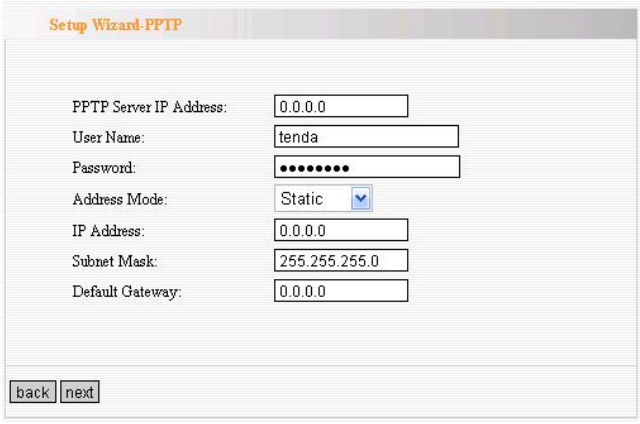
**Password:** Enter PPTP password provided by your ISP.

**Address Mode:** Select “Static” if your ISP supplies you with the IP address, subnet mask, and gateway. In most cases, select Dynamic.

**IP Address:** Enter the PPTP IP address supplied by your ISP.

**Subnet Mask:** Enter the Subnet Mask supplied by your ISP.

**Default Gateway:** Enter the Default Gateway supplied by your ISP.



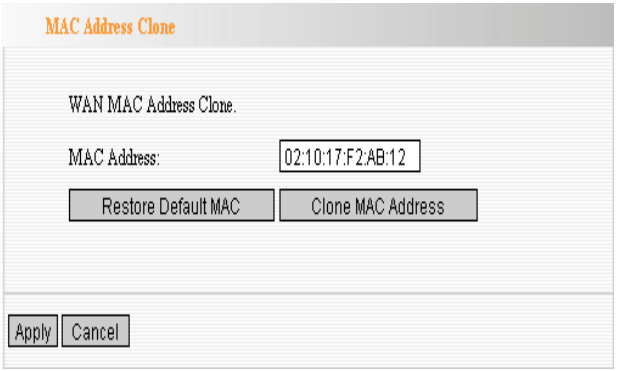
# MAC Address Clone

Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router.

**MAC Address:** The MAC address to be registered with your Internet service provider.

**Clone MAC address:** Register your PC's MAC address.

**Restore default MAC address:** Restore the default hardware MAC address.



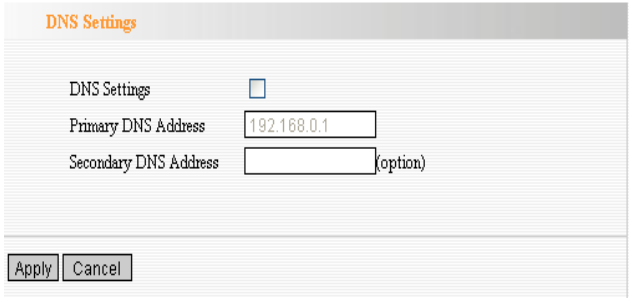
# DNS Settings

DNS is short for Domain Name System(or Service), an Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.

**DNS:**
Click the checkbox to enable the DNS server.

**Primary DNS Address:**
Enter the necessary address provided by your ISP.

**Secondary DNS Address:**
Enter the second address if your ISP provides, which is optional.



# Chapter 6: Wireless Settings

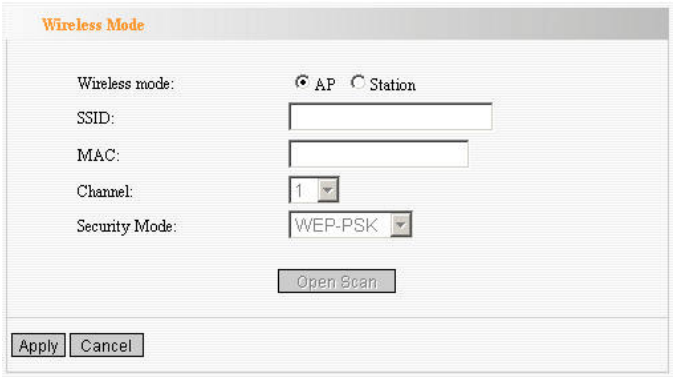
This section mainly deals with the wireless settings, including Basic Settings, Security Setting, Access Control and Advanced Settings.

## Wireless Mode

**AP Mode:** router serves as an access point in this mode to be connected. The work stations around will be connected with router by SSID to share the Internet resources. To configure the AP mode, open the Basic Setting and Security Setting windows in the Wireless Setting folder.

**Station Mode:** In this mode, router is used as a work station to be connected with an AP by scanning the AP's SSID and provides the security authentication. Generally speaking, AP mode is passive to be connected with work station, but Station mode always takes the initiative in connecting with AP.

**SSID:** SSID is the unique ID name of access point. The wireless work station must keep the same SSID name with the AP's for connections. By enabling Open Scanning button, the device can search available APs.



**MAC:** To connect certain AP, you need to know the AP's MAC address. By enabling Open Scanning button to find out the available AP's MAC address.

**Channel:** You can use the channel same as the AP. By enabling Open Scanning button to find out the available AP's channel.

**Security Mode:** router provides the following security authentication methods:

(1) WEP: selects ASCII format (5 or 13 ASCII characters except illegal characters.) or Hex format (10 or 26 Hex characters).

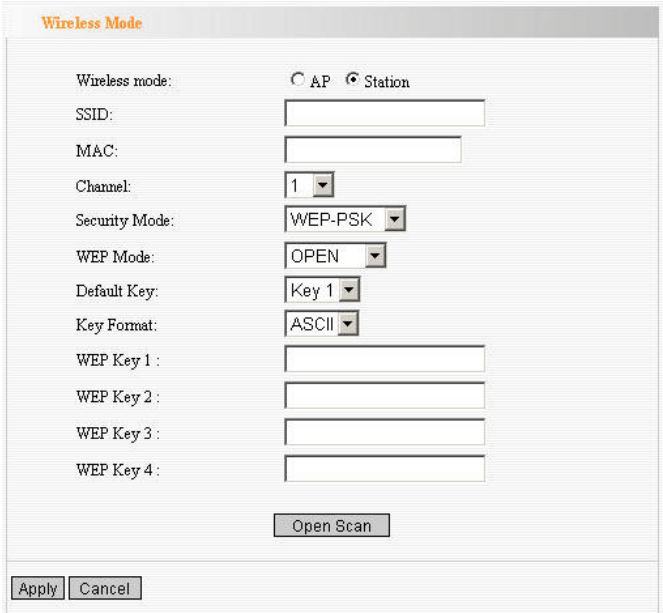
(2) WPA/WPA2-personal (PSK) is safer than other encryption methods because the key is subject to change all the time. WPA-PSK/WPA2-PSK utilizes the TKIP or AES encryption algorithm.

WEP Mode: The shared key requires the same WEP keys between the access point and work station.

**Default KEY:** After entering the WEP keys, select one key as the default one, for example, Key 1

**KEY Format:** AASCII: Enter 13 characters with case sensitive ("a-z", "A-Z" and "0-9"). Hex: enter 26 Hex characters ("A-F", "a-f" and “0~9”).

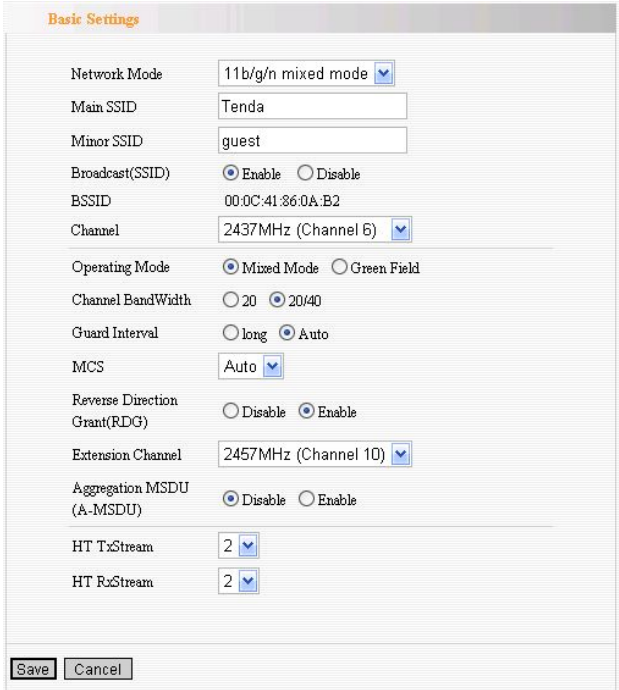
**KEY 1:** If the KEY 1 is selected as default key, the key will be enabled.



**KEY 2:** If the KEY 2 is selected as default key, the key will be enabled.
**KEY 3:** If the KEY 3 is selected as default key, the key will be enabled.
**KEY 4:** If the KEY 4 is selected as default key, the key will be enabled.
**WPA/WPA2 Algorithm:** When the WPA-PSK /WPA2-PSK authentication is selected, you can **select one from two:** TKIP and AES. For example, if the wireless provider selects TKIP, the wireless receiver (client) also needs to select TKIP for this authentication way.
**Password:** When WPA-PSK /WPA2-PSK authentication type is selected, enter the access password provided by AP users here.
**Apply:** Click “Apply” to make the settings go into effect.
**Cancel:** Click “Cancel” to throw all setting saved last time.

## Basic Settings

**Network Mode:** Supports 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed modes.
**Main SSID:** Main Service Set Identifier. It's the "name" of your wireless network.
**Minor SSID:** Minor Service Set Identifier. It is optional.
**Broadcast (SSID):** Select "enable" to enable the device's SSID to be visible by wireless clients.
**BSSID:** It is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP
**Channel:** From the drop-menu, it is for selecting the working channels of the wireless network. Please select from 1 to 13,or select AutoSelect to select different channels.
**Channel Bandwidth：** Select wireless work frequency 20M or 20/40M.
**HT TxStream:** RF Transmit Stream.
**HT RxStream:** RF Receive Stream.




## Wireless Security Settings

This page is to configure the wireless security of your Router. Six wireless security modes, WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise and RADIUS, are supported. If you do not want to use wireless security, select Disable from the drop-down menu.

# 1. Mixed WEP

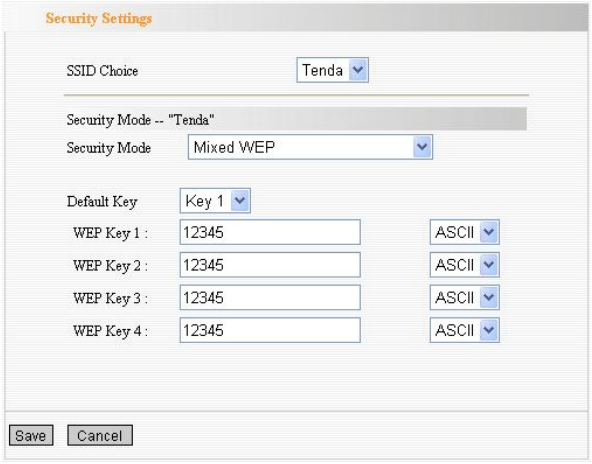
WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources.

**SSID Choice:** Select SSID to be configured security. The device supports to configure different security classes between the main SSID and the subordinate SSID.

**Security Mode:** There are several different security modes; you can choose one from mixed WEP, WPA-Personal, WPA-Enterprise, etc.

**Default Key:** Select a valid encryption key.

**WEP Key1, 2, 3, 4:** Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be **ASCII Characters** or **Hexadecimal Digits**



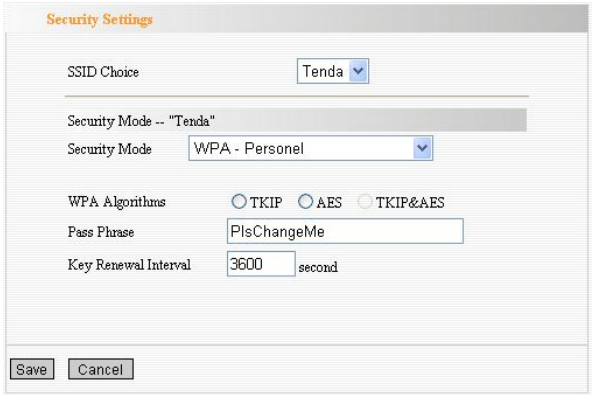
## 2. WPA-Personal

**WPA (Wi-Fi Protected Access)**, a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.

**WPA Algorithms:** Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

**Pass Phrase:** Enter the key which must have 8-63 ASCII characters.

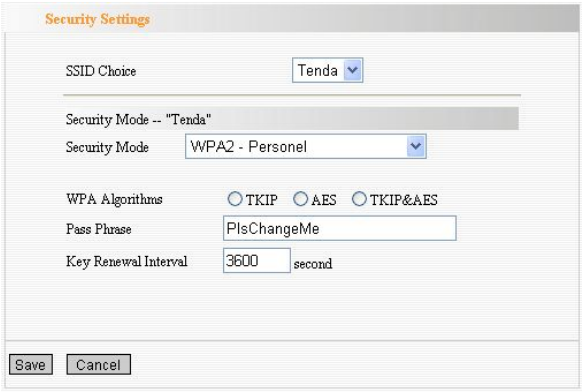
**Key Renewal Interval:** Enter the key renewal period. It is to tell the Router how often to change the keys.



## 3. WPA2-Personal

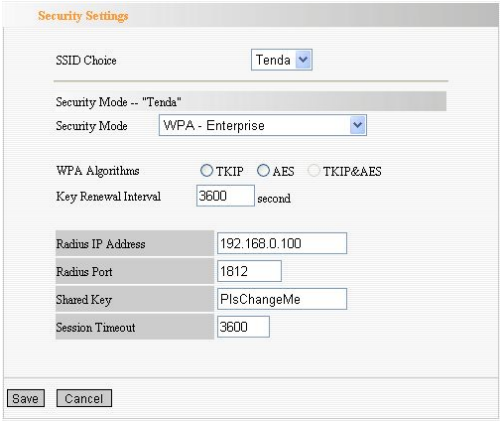
**WPA2 (Wi-Fi Protected Access version 2)**, It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.

**WPA Algorithms:** Select key Algorithms such as TKIP, AES and TKIP&AES.
**Pass Phrase:** Enter the key which must have 8-63 ASCII characters.
**Key Renewal Interval:** Enter the key renewal period. It is to tell the Router how often to change the keys.




## 4. WPA-Enterprise

This Authentication protocol based on RADIUS server. This security mode is used when a RADIUS server is connected to the Router.
**Radius IP Address:** Please input IP address of the radius server here.
**Radius Port:** Please input the port number of the radius server here.
**Shared key:** The encryption key that the router is authenticated through RADIUS server
**Session Timeout:** The recertification time interval between the router and the server. The default value is 3600s.



## 5. WPA2-Enterprise

This security mode is also used when a RADIUS server is connected to the Router.

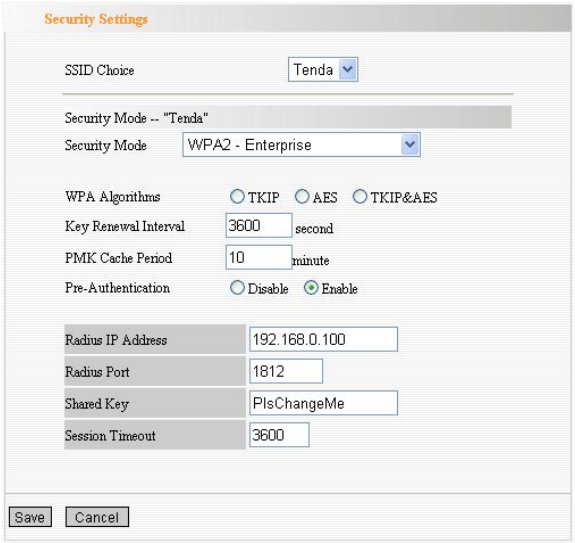
**WPA Algorithms:** Select key Algorithms such as TKIP and AES.

**Radius IP Address:** Please input IP address of the radius server here.

**Radius Port:** Please input the port number of the radius server here.

**Shared key:**The encryption key that the router is authenticated through RADIUS server

**Session Timeout:** The recertification time interval between the router and the server. The default value is 3600s.




## 6. 802.1X

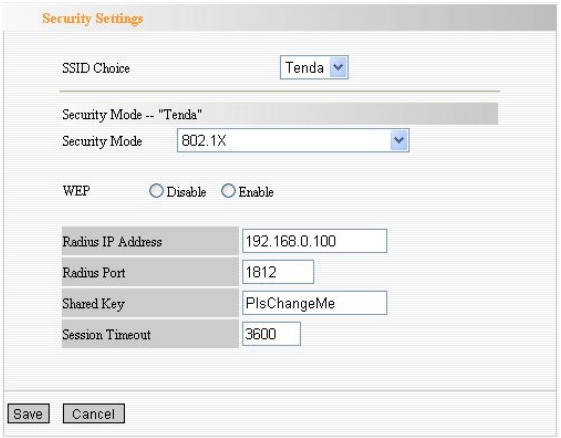
This security mode is used when a RADIUS server is connected to the Router. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass.

**WEP:** Select "enable/disable" WEP encryption which indicates the authentication process between wireless adapter and wireless router.

**Radius IP Address:** Please input IP address of the radius server here.

**Radius Port:** Please input the port number of the radius server here.

**Shared key:** The encryption key that the router is authenticated through RADIUS server.



**Session Timeout:** The recertification time interval between the router and the server. The default value is 3600s.

⚠***NOTE:*** ***To improve security level, do not use those words which can be found in a dictionary or too easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it's worth to use complicated WEP key to improve security level.***

## WPS Settings

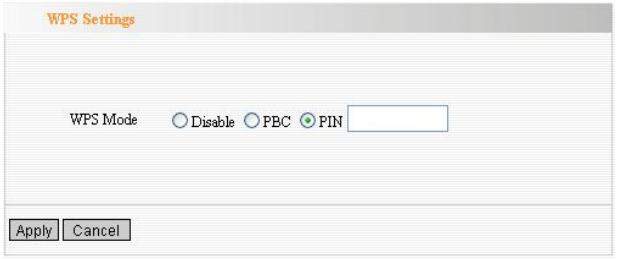
**WPS (Wi-Fi Protected Setting)** can be easy and quick to establish the connection between the wireless network clients and the Router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

**WPS Mode:** Supports two ways to configure WPS settings:

PBC (Push-Button Configuration) and PIN code.

**PBC:** Select the PBC or press the WPS button on the panel of the Router (Press the button for one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another Router to implement the WPS/PBC negotiation between them. At present, the WPS only support one client access. Two minutes later, the WPS indicator will be off.).

**PIN:** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the client.



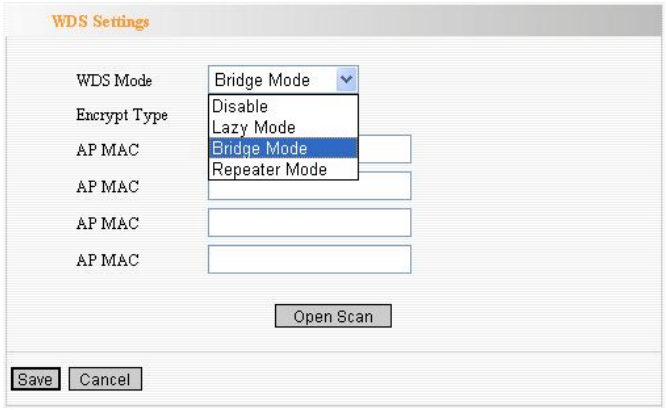

## WDS Settings

In this mode, you can expand the scope of network by combining up to four other access points together, and every access point can still accept wireless clients.

**Lazy Mode:** You need configure the router's BSSID into another device, not need input another router's BSSID in it, and then connect together automatically.

**Bridge Mode:** You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table. At the same time, the connecting device should be in Lazy, Repeater or Bridge mode.

**Repeater Mode:** You can select the mode to extend the distance between the two WLAN devices. Functioning as a WDS repeater, the W307R connects to both a client card as an AP and to another AP. In typical repeater applications, APs connecting to other APs equipped with WDS functionality must also support WDS. In this mode, you need to add the MAC address of the connecting device into the



Router's AP MAC address table and the connecting client should be in Lazy, Repeater or client mode.

**Encrypt Type:** You can select WEP mode, TKIP mode, AES mode for security here.

**Pass phrase:** Enter the key, the key format according to encryption you selected.

**AP MAC:** Input the MAC address of another wireless router.

⚠***NOTE*: *Two wireless routers must use the same band, channel number, and security setting!***

## Advanced Wireless Settings

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, Beacon Period and DTIM Interval.

**BG protection Mode:** Auto by default. You can select On or Off.

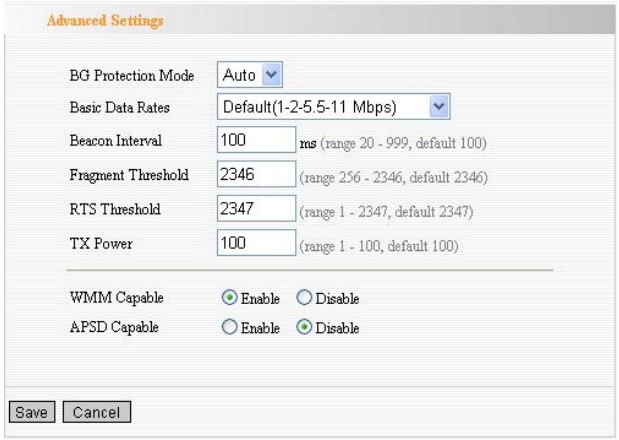
**Basic Data Rates:** For different requirement, you can select one of the suitable Basic Data Rates. Here, default value is (1-2-5.5.-11Mbps…).

**Beacon Interval:** Set the beacon interval of wireless radio. Do not modify default value if you don't know what it is, default value is 100.

**Fragment Threshold:** Do not modify default value if you don't know what it is, default value is 2346.

**RTS Threshold:** Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.

**TX Power:** You can set the output power of wireless radio. Unless you're using this wireless router in a really big space, you may not have to



set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).

**WMM Capable:** It will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is / not sure if you need it, it's safe to set this option to 'Enable', however, default value is enabling.

**APSD Capable:** It is used for auto power-saved service. The default is disabled.

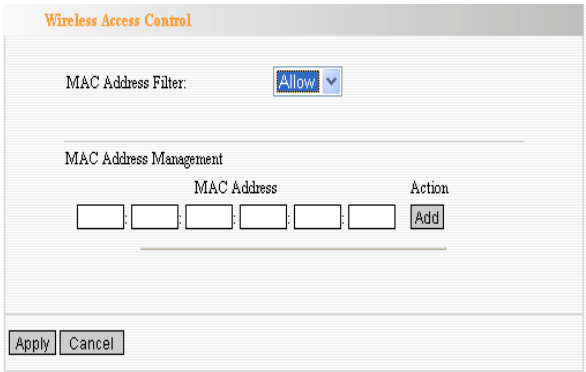
# Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management.

**MAC Address Filter:** If you want to access the Router from any external IP Address, please select the “Disable”.

**MAC Address:** To specify an external IP address, please add the MAC address manually and click “Add”.

**MAC Address List:** The added MAC addresses are listed here. Click “Delete” to delete the filter management for this MAC address.

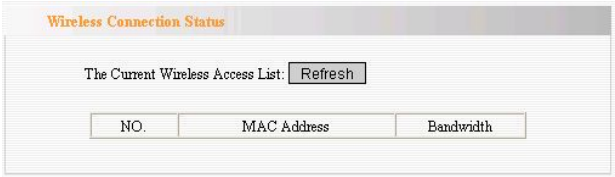


## Wireless Connection Status

This page is to show the current wireless access status. Click “Refresh” to update the wireless connection information.

**MAC Address:**
Shows the connecting PC’s MAC address.

**Bandwidth:** displays the channel bandwidth of the host to be connected.



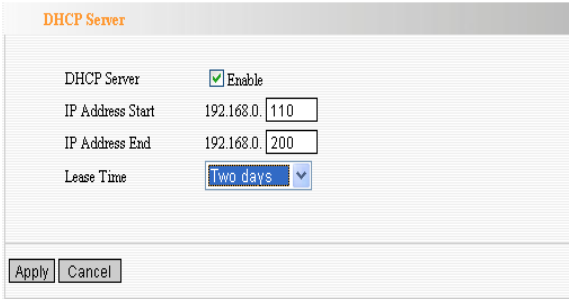
# Chapter 7: DHCP Server

**DHCP (Dynamic Host Control Protocol)** is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating “Obtain an IP Address Automatically”. So specifying the starting and ending address of the IP Address pool is needed.

**DHCP Server:** Activate the checkbox to enable DHCP server.

**IP Address Start/End:** Enter the range of IP address for DHCP server distribution.

**Lease Time:** The length of the IP address lease.



# DHCP Server List

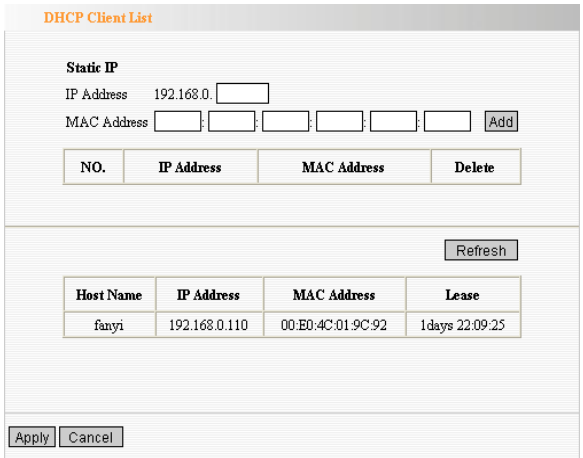
The Static IP assignment is to add a specifically static IP address to the assigned MAC address. You can view the related information in the DHCP server list.

**IP Address:** Enter one IP address for the computer on the LAN network.

**MAC Address:** Enter the MAC address of the computer you want to assign the above IP address. Click “Add” to add the entry in the list.

**Hostname:** The name of the computer which is added a new IP address.

**Lease Time:** The time length of the corresponding IP address lease.



# Chapter 8: Virtual Server

## Single Port Forwarding

The W307R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.

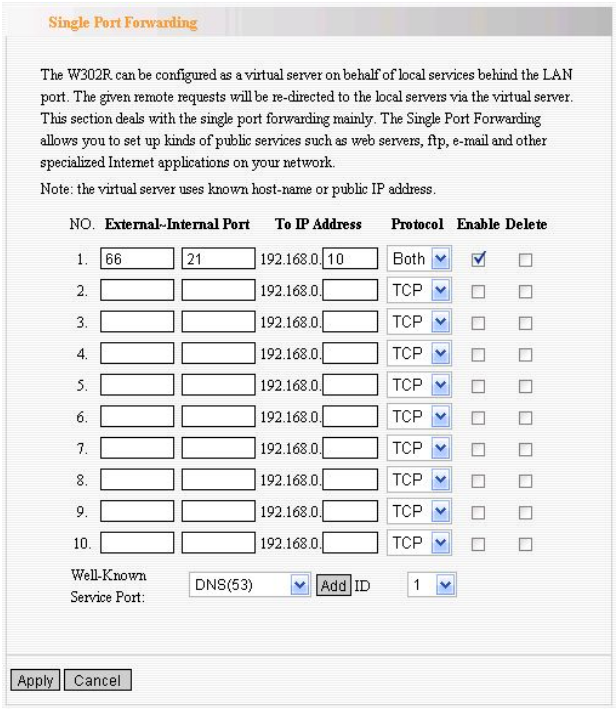
⚠ ***NOTE: <u>the virtual server uses known host-name or public IP address.</u>***

**External Port:** This is the external port number for server or Internet application, for example, port 21 for ftp service.

**Internal Port:** This is the port number of LAN computer set by the Router. The Internet traffic from the external port will forward to the internal port.

For example, you can set the internal port NO.66 to act as the external port NO.21 for ftp service.

**IP Address:** Enter the IP address of the PC


Single Port Forwarding
The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.
Note: the virtual server uses known host-name or public IP address.
NO. External--Internal Port To IP Address Protocol Enable Delete
1. 66 21 192.168.0. 10 Both
2. 192.168.0. TCP
3. 192.168.0. TCP
4. 192.168.0. TCP
5. 192.168.0. TCP
6. 192.168.0. TCP
7. 192.168.0. TCP
8. 192.168.0. TCP
9. 192.168.0. TCP
10. 192.168.0. TCP
Well-Known Service Port: DNS(53) Add ID 1
Apply Cancel

where you want to set the applications.

**Protocol:** Select the protocol (TCP/UDP/Both) for the application.

**Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

**Delete/Enable:**Click to check it for corresponding operation.

⚠***NOTE***: ***If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.***

# Port Range Forwarding

This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.

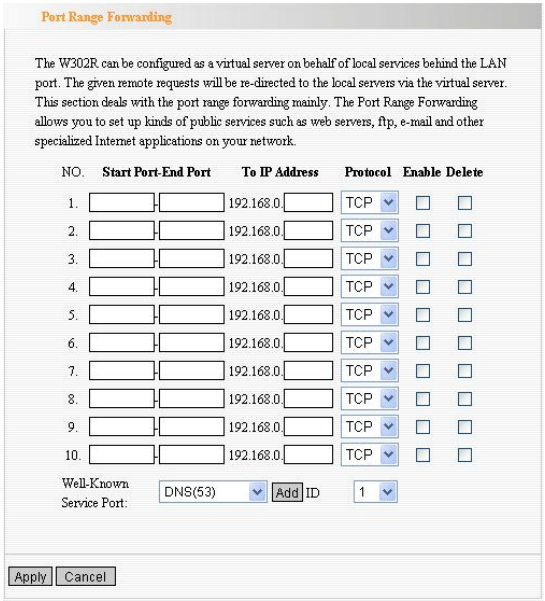
**Start/End Port:** Enter the start/end port number which ranges the External ports used to set the server or Internet applications.

**IP Address:** Enter the IP address of the PC where you want to set the applications.

**Protocol:** Select the protocol (TCP/UDP/Both) for the application.

**Well-Known Service Port:** Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

**Delete/Enable:**Click to check it for corresponding operation.


Port Range Forwarding
The W302R can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.
NO. Start Port-End Port To IP Address Protocol Enable Delete
1. 192.168.0. TCP
2. 192.168.0. TCP
3. 192.168.0. TCP
4. 192.168.0. TCP
5. 192.168.0. TCP
6. 192.168.0. TCP
7. 192.168.0. TCP
8. 192.168.0. TCP
9. 192.168.0. TCP
10. 192.168.0. TCP
Well-Known Service Port: DNS(53) Add ID 1
Apply Cancel

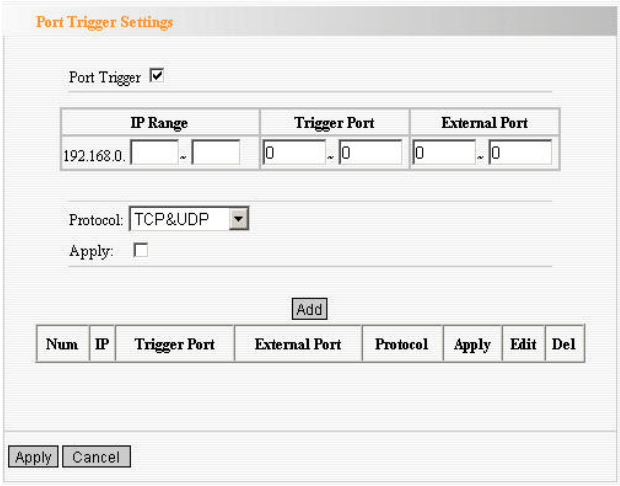
# Port Trigger Settings

When internal clients have access to external server in the Internet for some application, the clients request to connect with severs, and the server will also ask to connect with client. But in the default setting, router will refuse to accept any request from WAN, which will bring communication halt. The **port triggering** is used to define triggering rules. So when clients have access to the server, the device will open the port through which the server sends the request to client.

**IP Range:** The internal IP address range for requesting external server application.

**Trigger Port:** The port range through which the internal clients send request traffics to external server with the range of 1～65535. Note that the low number first and two blanks can keep the same number if needed.

**External Port:** The port range through which the external server send request traffics to internal clients with the range of 1～65535. Note that the low number first and two blanks can keep the



same number if needed.

**Apply:** To enable or disable the rule.

**Add:** After edit the rule, click the “add” button to add the current entry to port triggering list.

**Apply:** Click “Apply” to activate the current rule.

**Cancel:** Click “Cancel” to drop all setting saved last time.

It is allowed to delete or modify the previous rules in the list table.

**Note: The special application can be only used in one PC. If there is more than one PC to open the same triggering port, the external port will be connected to the last PC for the application.**

# ALG Service Settings

**ALG(Application Layer Gateway)**

In the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer applications etc.

In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

Usually allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the

server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.

In the default ALG settings, the following protocols have enabled. **It is recommended to keep the settings unchanged.**

1,FTP
2,TFTP
3,PPTP
4,IPSec
5,L2TP

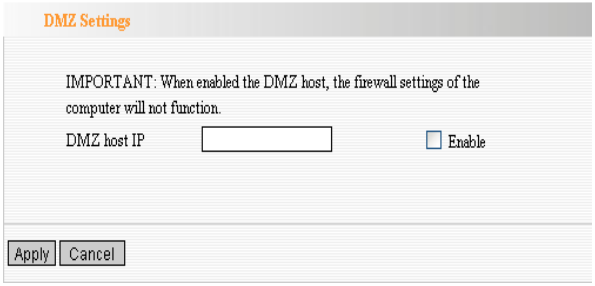
## DMZ Settings

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.

**DMZ Host IP Address:** The IP address of the computer you want to expose.

**Enable:** Click the checkbox to enable the DMZ host.

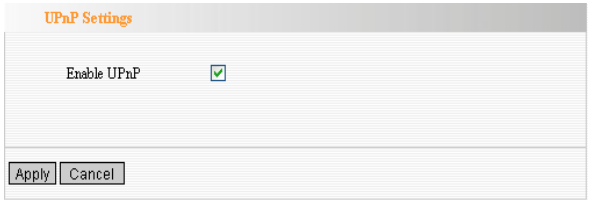
***IMPORTANT:*** ***When enabled the DMZ host, the firewall settings of the DMZ host will not function.***




## UPnP Settings

It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.

**Enable UPnP:** Click the checkbox to enable the UPnP.



# Chapter 9: Traffic Control

## Traffic Control

**Traffic control** is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.

**Enable Traffic Control:** To enable or disable the internal IP bandwidth control.

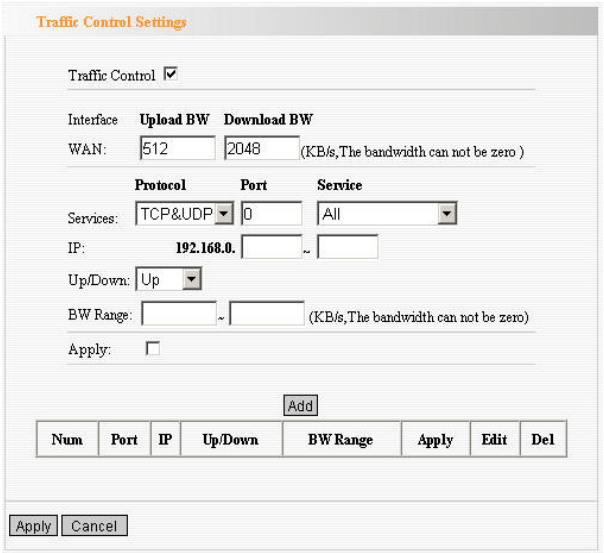
**Interface:** To limit the uploading and downloading bandwidth in WAN port.

**Service:** To select the controlled service type, such as HTTP service.

**IP Starting Address:** The first IP address for traffic control.

**IP Ending Address:** The last IP address for traffic control.

**Uploading/Downloading:** To specify the



traffic heading way for the selected IP addresses: uploading or downloading.

**Bandwidth:** To specify the uploading/downloading Min. /Max. Traffic speed (KB/s), which can not exceed the WAN speed.

**Apply:** To enable the current editing rule. If not, the rule will be disabled.

**Add:** After edit the rule, click the “add to list” button to add the current rule to rule list.

**Apply:** Click “Save” to activate the current rule.

**Cancel:** Click “Cancel” to drop all setting saved last time.

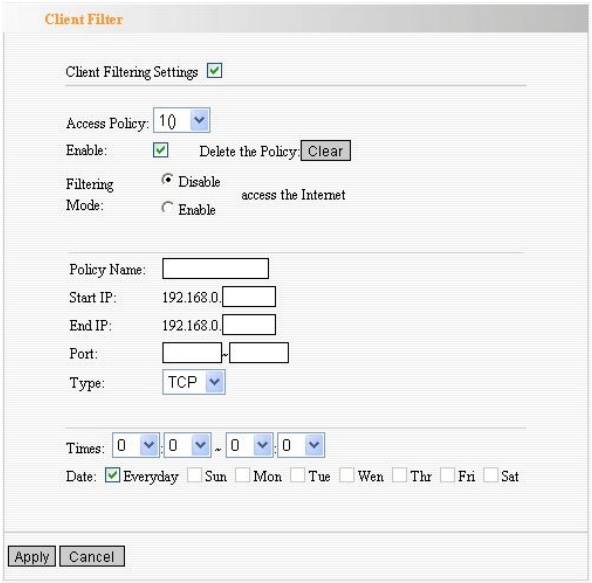
**It is allowed to delete or modify the previous rules in the list table.**

# Chapter 10: Security Settings

## Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.

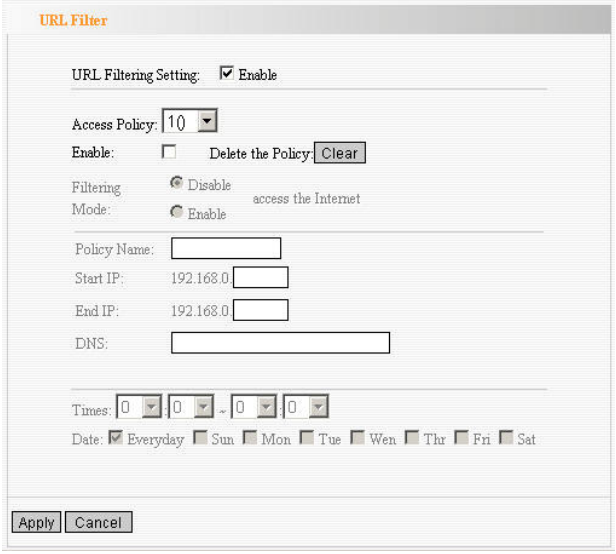
**Client Filter:** Check to enable client filter.
**Access Policy:** Select one number from the drop-down menu.
**Enable:** Check to enable the access policy.
**Clear the Policy:** Click “Clear” button to clear all settings for the policy.
**Filter Mode:** Click one radio button to enable or disable to access the Internet.
**Policy Name:** Enter a name for the access policy selected.
**IP Start/End:** Enter the starting/ending IP address.
**Port No.:** Enter the port range based over the protocol for access policy.
**Protocol:** Select one protocol (TCP/UDP/Both) from the drop-down menu.
**Times:** Select the time range of client filter.
**Days:** Select the day(s) to run the access policy.



# URL Filter Settings

In order to control the computer to have access to websites. You can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.

**URL Filter:** Check to enable URL filter.
**Access Policy:** Select one number from the drop-down menu.
**Enable:** Check to enable the access policy.
**Clear the Policy:** Click “Clear” button to clear all settings for the policy.
**Filter Mode:** Click one radio button to enable or disable to access the Internet.
**Policy Name:** Enter a name for the access policy selected.
**Start/End IP:** Enter the starting/ending IP address.
**DNS:** Specify the text strings or keywords in the DNS. If any part of the URL contains these strings or words, the web page will not be accessible and display.
**Times:** Select the time range of client filter.
**Days:** Select the day(s) to run the access policy.



# MAC Address Settings

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.

**MAC Address Filter:** Check to enable MAC address filter.

**Access Policy:** Select one number from the drop-down menu.

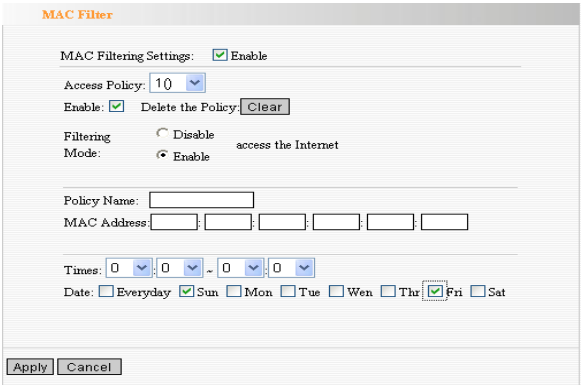
**Enable:** Check to enable the access policy.

**Clear the Policy:** Click "Clear" button to clear all settings for the policy.

**Filter Mode:** Click one radio button to enable or disable to access the Internet.

**Policy Name:** Enter a name for the access policy selected.

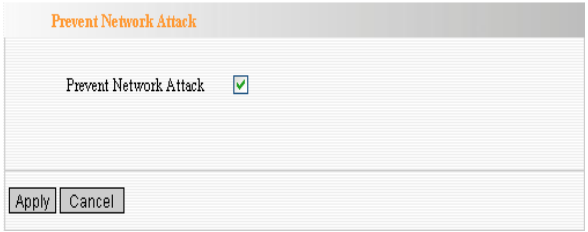
**MAC Address:** Enter the MAC address you want to run the access policy.
**Times:** Select the time range of client filter.
**Days:** Select the day(s) to run the access policy.


MAC Filter
MAC Filtering Settings: Enable
Access Policy: 10
Enable: Delete the Policy: Clear
Filtering Mode: Disable Enable access the Internet
Policy Name:
MAC Address:
Times: 0 : 0 ~ 0 : 0
Date: Everyday Sun Mon Tue Wen Thr Fri Sat
Apply Cancel

## Prevent Network Attack

This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically.
The attacker's IP address can be found from the "System Log".

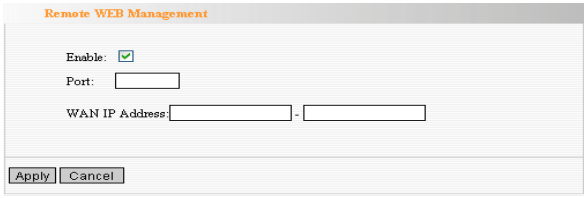
**Prevent Network Attack:** Check to enable it for attack prevention.




## Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the "Enable".

**Enable:** Check to enable remote web management.
**Port:** The management port open to outside access The default value is 80.
**WAN IP Address:** Specify the range of the WAN IP address for remote management.

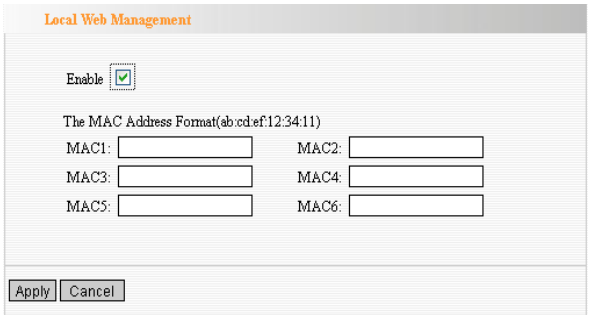


## Local Web Management

**Local web management**, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.

**Enable:**
Check to enable the local web management

**MAC1/2/3…:**
Enter the MAC addresses of LAN computers.




## WAN Ping

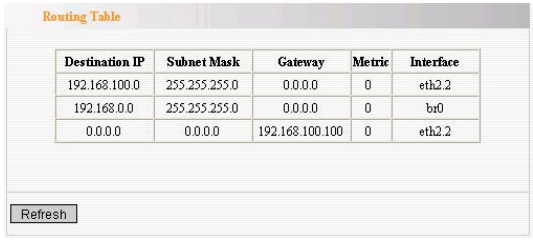
The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.

**Disable the Ping for WAN:** Check to enable it.

# Chapter 11: Routing Settings

## Routing Table

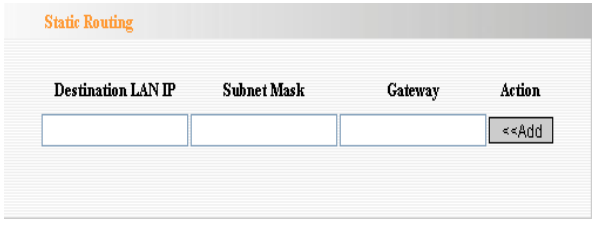
The main duty for router is to look for a best path for every data frame, and transfer this data frame to destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.




## Static Route

Static Route is set by administrator in advance is called static route. Usually, it is set according to network configuration when installing the operation system. It would not be changed according to network structure's change.

**Destination LAN IP:** The address of the remote host with which you want to construct a static route.
**Subnet Mask:** The network portion of the Destination LAN IP.
**Gateway:** The gateway of the next hop.

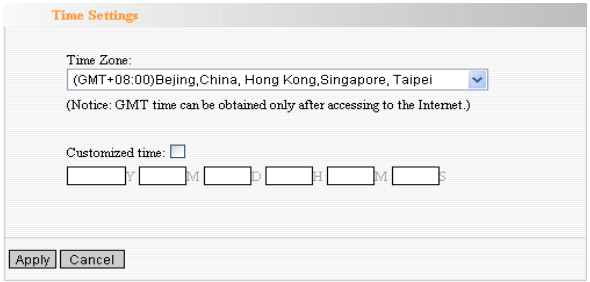


# Chapter 12: System Tools

## Time

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.

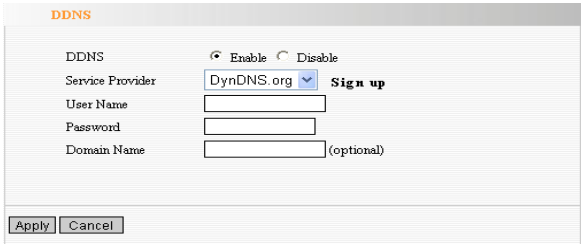
**Time Zone:** Select your time zone from the drop-down menu.
**Customized time:** Enter the time you customize.


Time Settings
Time Zone:
(GMT+08:00)Bejing,China, Hong Kong,Singapore, Taipei
(Notice: GMT time can be obtained only after accessing to the Internet.)
Customized time:
Y M D H M S
Apply Cancel

## DDNS

The **DDNS (Dynamic Domain Name System)** is supported in this router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select “Enable” and a DDNS service provider to sign up.

**DDNS:** Click the radio button to enable or disable the DDNS service.
**Service Provider:** Select one from the



drop-down menu and press “Sign up” for registration.

**User Name:** Enter the user name the same as the registration name.

**Password:** Enter the password you set.

**Domain Name:** Enter the domain name which is optional.

## Backup/Restore

The device provides backup/restore settings, so you need set a directory to keep these parameters.

**Backup:** Click this button to back up the Router’s configurations.

**Browse:** Click this button to browse the directory where you Back up or save files.

**Restore:** Click this button to restore the Router’s configurations.

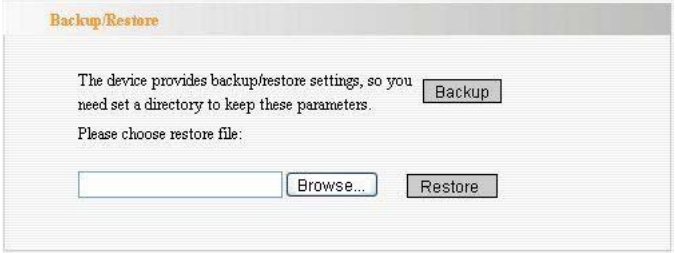
# Firmware Upgrade

The Router provides the firmware upgrade by clicking the “Upgrade” after browsing for the firmware upgrade packet which you can download from www.tenda.cn. After the upgrade is completed, the Router will reboot automatically.

**Browse:** Click this button to browse the directory where you download the firmware upgrade files.

**Upgrade:** Click this button to start upgrade.

***IMPORTANT:*** ***Do not power off the system during the firmware upgrade to avoid damaging the device. The Router will reboot after the upgrade.***



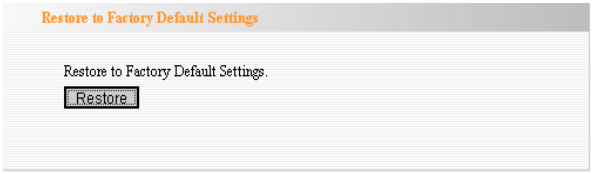
# Restore to Factory Default Settings

This button is to reset all configurations to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.

**Restore to Factory Default Settings:** Click this button to restore to default settings.

Factory Default Settings:
User Name: **admin**
Password: **admin**
IP Address: **192.168.0.1**
Subnet Mask: **255.255.255.0**

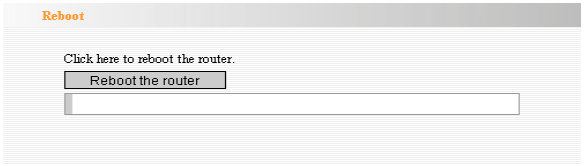
⚠ ***NOTE: After restoring to default settings, please restart the device, then the default settings can go into effect.***



## Reboot

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.

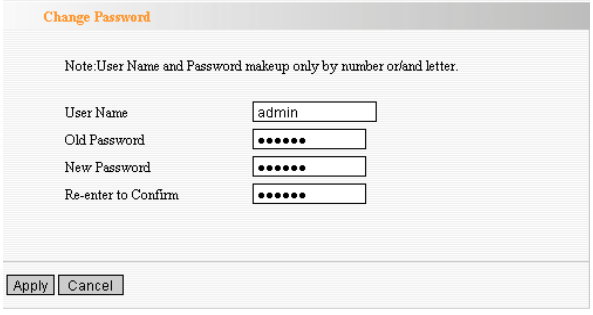
**Reboot the router:** Click this button to reboot the device.




## Change Password

This section is to set a new user name and password to better secure your router and network. Please Note that the new password should be less than 14 characters.

**User Name:** Enter a new user name for the device.
**Old Password:** Enter the old password.
**New Password:** Enter a new password.
**Re-enter to Confirm:** Re-enter to confirm the new password.
⚠***NOTE:*** ***<u>It is highly recommended to change the password to secure your network and the Router.</u>***

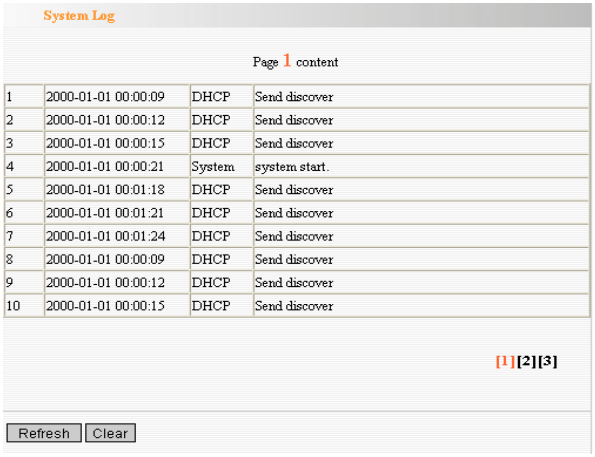


# System Log

The section is to view the system log. Click the “Refresh” to update the log. Click “Clear” to clear all shown information. If the log is over 150 records, it will clear them automatically.

**Refresh:** Click this button to update the log.

**Clear:** Click this button to clear the current shown log.


System Log
Page 1 content
1 2000-01-01 00:00:09 DHCP Send discover
2 2000-01-01 00:00:12 DHCP Send discover
3 2000-01-01 00:00:15 DHCP Send discover
4 2000-01-01 00:00:21 System system start.
5 2000-01-01 00:01:18 DHCP Send discover
6 2000-01-01 00:01:21 DHCP Send discover
7 2000-01-01 00:01:24 DHCP Send discover
8 2000-01-01 00:00:09 DHCP Send discover
9 2000-01-01 00:00:12 DHCP Send discover
10 2000-01-01 00:00:15 DHCP Send discover
[1][2][3]
Refresh
Clear

# Appendix A: Product Features

◆Integrates router, wireless access point, four-port switch and firewall in one
◆Complies with IEEE802.11n, IEEE802.11b and IEEE802.11g standards
◆MIMO technology utilizes reflection signal to increase eight times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
◆Provides 300Mbps receiving rate and 150Mbps sending rate
◆Supports WMM to make your voice and video more smooth
◆Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standards
◆WPS (PBC and PIN) encryption method to free you from remembering long passwords
◆Supports remote/local Web management
◆Supports wireless Roaming technology and ensures high-efficient wireless connections
◆Supports wireless SSID stealth mode and MAC address access control
◆Supports Auto MDI/MDIX
◆Provides system log to record the status of the router
◆Supports MAC address filtering, NAT, NAPT
◆Supports UPnP and DDNS
◆Supports the access control over 30 MAC addresses
◆Supports DHCP server/client
◆Supports SNTP
◆Supports virtual server and DMZ host
◆Supports auto wireless channel selection
◆Supports WDS function (wireless distribution system)